FORTINET
High Performance Network Security

FortiToken Comprehensive Guide

FortiToken-200, FortiToken-200CD, FortiToken-220, FortiToken Mobile, FortiGate/FortiOS 5.4, and FortiAuthenticator 4.2

FORTIOS
5.4
VERSION

FORTINET DOCUMENT LIBRARY

http://docs.fortinet.com

FORTINET VIDEO GUIDE

http://video.fortinet.com

FORTINET BLOG

https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT

https://support.fortinet.com

http://cookbook.fortinet.com/how-to-work-with-fortinet-support/

FORTIGATE COOKBOOK

http://cookbook.fortinet.com

FORTINET TRAINING SERVICES

http://www.fortinet.com/training

FORTIGUARD CENTER

http://www.fortiguard.com

END USER LICENSE AGREEMENT

http://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK

Email: techdocs@fortinet.com

Thursday, December 15, 2016

FortiToken Comprehensive Guide

33-100-365829-20160324

TABLE OF CONTENTS

Change Log

Date	Change Description
2016-12-15	Added FortiToken Mobile 4.0 new feature information: PUSH notifications and Touch ID.
2016-10-04	Added information regarding FortiToken authentication with no Internet.
2016-08-22	Clarified CLI command information regarding activation code expiry.
2016-07-18	Added information regarding FortiToken deployment in an HA cluster with multiple FortiGate/FortiAuthenticator units.
2016-06-06	Added video link to the configuration example "IPsec VPN two-factor authentication with FortiToken-200".
2016-06-01	Added information in Reference section regarding FortiToken provisioning with FortiAuthenticator REST API.
2016-05-12	Added video link to the configuration example "Captive portal WiFi access with FortiToken-200".
2016-03-24	Initial release. This release combines previous related FortiToken documentation into a single resource.

Introduction

FortiTokens are security tokens used as part of a two-factor authentication system on FortiGate/FortiOS and FortiAuthenticator devices. The token produces a temporary six or eight digit (configurable) code that is used to prove one's identity electronically as a prerequisite for accessing network resources. There are many types of hardware and software based tokens, sometimes referred to as dongles, key fobs, authentication tokens, USB tokens, and cryptographic tokens.

FortiToken is available as either a physical or a mobile token, as described below.

For the purposes of this document, FortiOS version 5.4.0 build1011 (GA) and FortiAuthenticator version v4.2 build0143-20161101-patch00 (GA) was used.

Physical token

- **FortiToken-200:** These physical tokens display their code on the device itself, and provide two-factor authentication for RADIUS, LDAP, and 802.1X wireless authentication, as well as Fortinet Single Sign-on (FSSO). This kind of two-factor authentication improves security by moving away from use of static passwords.

  FortiToken-200 can only be transferred from one FortiGate or FortiAuthenticator device to another by contacting customer support.

When contacting customer support, you must provide the FortiToken serial number, as well as the FortiGate or FortiAuthenticator serial number to which the token is assigned.

- **FortiToken-200CD:** These tokens provide the same authentication properties as FortiToken-200 devices, however they come with an activation CD. The CD contains the token seed files which are installed to the FortiGate or FortiAuthenticator, and is used to easily import multiple FortiTokens at once.

  Because the token seed files are stored on the CD, these tokens can be registered on multiple FortiGates and/or FortiAuthenticators but not simultaneously.

- **FortiToken-220-Edge:** These tokens provide the same authentication properties as FortiToken-200 devices, however they come in a convenient mini credit card form factor. The FTK220 uses NFC technology so you have the option to program the seeds for your Edge on your own using our programmer application on your smartphone.

Mobile token

- **FortiToken Mobile:** These tokens produce their codes in an application you can download to your Android or iOS device that is used just like a FortiToken-200 but without the need for a physical token. FTM uses push technology so you can receive login attempt notifications on your smartphone or tablet and verify the login with a single tap.

  For the purposes of this document, FTM iOS version 4.0 was used.

How this guide is organized

This guide contains the following sections:

Administrator guide

- Setting up FortiToken Hardware
- Registering and provisioning FortiToken Mobile tokens
- Deactivating a FortiToken
- Considerations

Configuration examples

- Example - Two-factor authentication with captive portal
- Example - IPsec VPN two-factor authentication with FortiToken-200
- Example - Captive portal WiFi access with FortiToken-200
- Example - FortiToken two-factor authentication with RADIUS on a FortiAuthenticator
- Example - Third-party token activation with Google

Reference

- FortiToken platform scalability
- Drift adjustment
- Diagnosing FortiToken on the FortiGate

Administrator guide

The following sections demonstrate how to set up FortiToken support for your end users on either a FortiGate or a FortiAuthenticator.

Setting up FortiToken Hardware

The following steps are required to add FortiToken two-factor authentication to a user on the FortiGate or FortiAuthenticator:

- Registering FortiToken-200/200CD/220-Edge
- Assigning the FortiToken to the user

The FortiGate must also have a FortiGuard subscription to support FortiToken.

Registering a FortiToken

The following steps show how to register a FortiToken-200, FortiToken-200CD, and FortiToken-220-Edge on a FortiGate and FortiAuthenticator.

On the FortiGate

1. Go to **User & Device > FortiTokens** and select **Create New**.
2. Set **Type** to **Hard Token** and enter the FortiToken serial number in the **Serial Number** field, then select **OK**.

If you have several FortiTokens to add at once, you can list their serial numbers in a text file and select **Import**. Each serial number must be listed individually per line of text.

3. Wait for the FortiGuard to validate your FortiToken's serial number. When you first enter the serial number, its status is listed as **Pending**. When FortiGuard validates the serial number, the status changes to **Available**.

Follow the same procedure above for both FortiToken-200 and FortiToken-220-Edge units.

For FortiToken-200CD:

1. Insert the activation CD labeled **FortiToken-200 Activation File**.
2. Go to **User & Device > FortiTokens** and select **Create New**. Set **Type** to **Hard Token** and select **Import**.
3. Select **Seed File**, browse to the CD and select the .FTK file, then select **OK**.
4. Each FortiToken will be installed and activated.

On the FortiAuthenticator

1. Go to **Authentication > User Management > FortiTokens** and select **Create New**.
2. Set **Token type** to **FortiToken hardware** and enter the FortiToken serial number in the **Serial numbers** field, then select **OK**.

If you have several FortiTokens to add at once, you can select **Import Multiple** and import by **Serial number file**, **Seed file**, or **FortiGate configuration file**.

For FortiToken-200CD:

1. Insert the activation CD labeled **FortiToken-200 Activation File**.
2. Go to **Authentication > User Management > FortiToken** and select **Import**. Set **File type** to **Seed file**, browse to and select the .FTK file on the CD, and select **OK**.
3. Each FortiToken will be installed and activated.

Assigning a FortiToken to a user

The following steps show how to assign a FortiToken to a user on a FortiGate and FortiAuthenticator.

On the FortiGate

1. Go to **User & Device > User > User Definition** and edit a user.
2. Enable **Two-factor Authentication** and select the FortiToken from the list. Select **OK**.
3. Go back to **User & Device > FortiTokens** to confirm that the FortiToken is assigned to the user you edited.

On the FortiAuthenticator

1. Go to **Authentication > User Management > Local Users** and edit a user.
2. Enable **Token-based authentication**, select **FortiToken**, and select the FortiToken from the dropdown menu. Select **OK**.
3. Go back to **Authentication > User Management > FortiTokens** to confirm that the FortiToken is assigned to the user you edited.

Registering and provisioning FortiToken Mobile tokens

To deploy FortiToken Mobile for your end users, you must first register the tokens on your FortiGate or FortiAuthenticator. After registering the tokens, you can assign them to your end users.

Platforms that support FortiToken Mobile:

Platform	Device and Firmware support
Android	• Smartphones and tablets • Firmware version Jellybean 4.1+

Platform	Device and Firmware support
iOS	• iPhone, iPad, and iPod Touch • Firmware version iOS 6.0+
Windows Phone	• Windows 10 Mobile, Windows Phone 8.1, and Windows Phone 8.

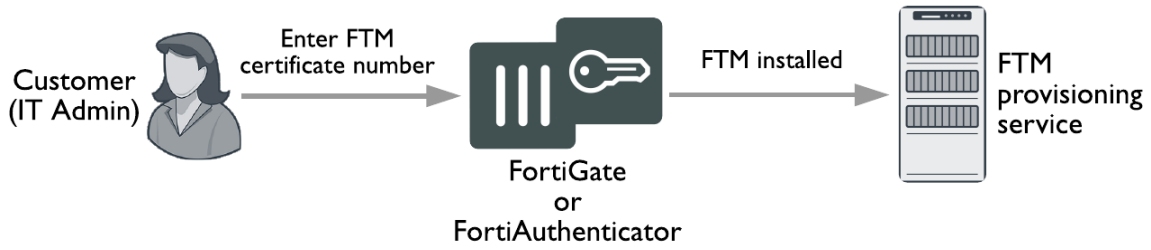
You will need a certificate to register FortiToken Mobile. There are two options for getting FortiToken Mobile certificates for use on your authentication server: FortiToken Mobile Redemption Certificate, and FortiToken Mobile Free Trial “virtual” certificate.

For each FortiToken Mobile purchase, you will receive a physical redemption certificate. Scratch off the designated area of the redemption certificate to reveal the 20-digit activation code.

Each FortiGate or FortiAuthenticator device also comes with a trial license for two free trial tokens. The device must be registered with FortiCare to retrieve the tokens. The certificate code to use for the free trial FortiToken Mobile tokens is 0000-0000-0000-0000-0000.

The registration process is the same for the Redemption Certificate and the Free Trial Tokens:

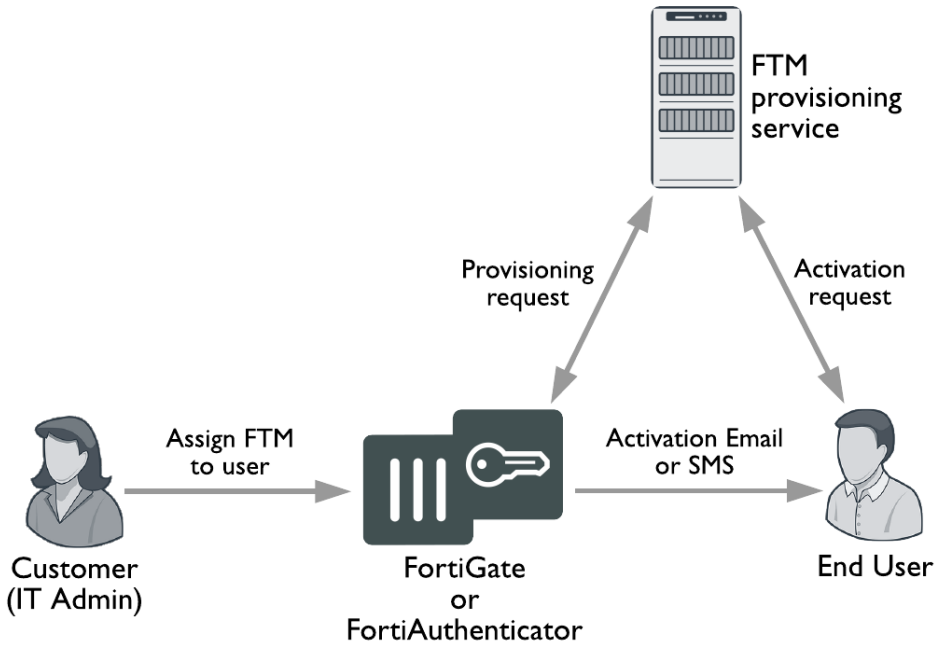
1. The authentication server administrator enters the certificate activation code from the Redemption certificate.
2. The authentication server sends the activation code to the FortiToken Mobile provisioning server, which validates the request, registers the FortiToken Mobile license, and sends the FortiToken Mobile serial numbers back to the authentication server.



The provisioning process includes the following steps:

1. A FortiToken Mobile token must be assigned to the user by an authentication server administrator.
2. The authentication server notifies the provisioning server that the token has been assigned for subsequent activation and receives back an activation code to forward to the end user.
3. The end user will receive an activation notification via email or SMS, depending on how the authentication server is configured.

   After registering the FortiToken Mobile on the mobile device, the end user can activate the token anytime within a configurable provisioning time period and begin generating their six-digit authentication codes.



PUSH Notifications

The release of FortiToken Mobile 4.0 updates the application to support PUSH notifications and Touch ID as an optional choice over using a PIN, allowing an extra layer of security.

PUSH notifications are used to send alerts to the end-user's device each time a login request is made. The alert contains information about the login attempt, for example the location from which the attempt originated. The user simply taps to approve or deny the request. If approved, a new OTP is automatically generated and sent by FortiToken Mobile to transparently authenticate the end-user in the background. If denied, FortiToken Mobile automatically sends an alert to the System Administrator.

The manual OTP authentication method is still available in case the end-user cannot or does not wish to use PUSH.

When upgrading, users will see a request to allow notifications. This is required for PUSH notifications to work.

Registering FortiToken Mobile

The following steps show how to register FortiToken Mobile on a FortiGate and FortiAuthenticator.

On the FortiGate

1. Locate the 20-digit code on the redemption certificate.
2. Go to **User & Device > FortiTokens** and select **Create New**.
3. Select **Mobile Token**, and enter the 20-digit certificate code in the **Activation Code** box.
4. Select **OK**.

On the FortiAuthenticator

1. Locate the 20-digit code on the redemption certificate.
2. Go to **Authenticaton > User Management > FortiTokens** and select **Create New**.
3. Select **FortiToken Mobile**, and enter the 20-digit certificate code in the **Activation codes** box.
4. Select **OK**.

Provisioning FortiToken Mobile

To ensure messaging functions properly, you must configure the messaging server, configure users to receive messages from the server by email or SMS, and use the FortiToken Mobile token.

The following steps show how to provision FortiToken Mobile for a user on a FortiGate and FortiAuthenticator.

On the FortiGate

1. Go to **System > Advanced**.
2. Configure the server under **Email Service** as required (note that port 25 is the default port).
3. Go to **User & Device > User Definition**.
4. Edit the user you wish to assign the FortiToken Mobile.
5. Select **Enable Two-factor Authentication** and select the FortiToken Mobile from the dropdown menu.
6. Under **Contact Info**, enable **Email Address** or **SMS**, enter the user's contact information, and select **Send Activation Code Email** or **Send Activation Code SMS**.

   The user will receive the activation code by the method specified.
7. Open the FortiToken Mobile application and go to **Add account > Enter Manually > Fortinet**.
8. Enter your email address, enter the activation code you received, and tap **Add account**.

   Your token will activate and start generating codes.

Alternatively, use the attached QR code if you chose to have your activation code sent to you by email. Activate the token with the **Scan Barcode** option instead of **Enter Manually**.

Activation CLI

The activation code will expire after a configurable time period. To configure the time period for FortiToken Mobile, use the following CLI command:

```
config system global
   set two-factor-ftm-expiry <time-in-hours>
end
```

To configure the time period for physical FortiTokens, use the following CLI command:

```
config system global
   set two-factor-ftk-expiry <time-in-hours>
end
```

The `time-in-hours` value should be in the range of 1 to 168.

The CLI command above should be used *instead* of `set activation-expire` under `config user fortitoken`.

The CLI command `set activation-code`, under `config user fortitoken`, cannot be used/set by the administrator.

On the FortiAuthenticator

1. Go to **System > Messaging > SMTP Servers** and select **Create New**.
2. Configure the server as required:

Name	Enter a name to identify this mail server on the FortiAuthenticator unit.
Server name/IP	Enter the IP address or Fully Qualified Domain Name (FQDN) of the mail server.
Port	The default port is **25**. Change it if your SMTP server uses a different port.
Sender email address	Enter the email address that will appear when sending an email from the FortiAuthenticator unit.
Secure connection	For a secure connection to the mail server, select **STARTTLS** from the drop-down list. Note that the necessary CA certificate must be imported for STARTTLS to work.
Enable authentication	Select if the email server requires you to authenticate when sending an email. Enter the **Account username** and **Password** if required.

3. Go to **System > Administration > FortiGuard**.
4. Under **FortiToken Mobile Provisioning**, ensure that the **Activation timeout** period is set. This is the time period in hours (1 to 168) in which the end user must activate the token before having to re-provision the token.
5. Go to **Authentication > User Management > Local Users** and select **Create New**.
6. In the **Password creation** dropdown menu, select **No password, FortiToken authentication only**, and select **OK**.
   Note: Only after you select **OK** can you specify a token and enter contact information for the user.
7. Once created, the user account will become disabled. You must associate a FortiToken and re-enable it. Deselect the **Disabled** radio, and select **Token-based authentication**. Choose to deliver the token by **FortiToken** and select an available **FortiToken Mobile** token from the dropdown menu.
8. Under **User Information**, enter the user's **Email address**. You may also enter their **Mobile number**.
9. Select **OK**.

Deactivating a FortiToken

You can deactivate a FortiToken by removing the token from the user to which it is assigned.

On the FortiGate

1. Go to **User & Device > User Definition**, and edit the user for which you want to deactivate the token.
2. Deselect **Enable Two-factor Authentication**, and select **OK**.
   The token will be removed from the user's **Two-factor authentication** column. The user will also be removed from the token's **User** column, under **User & Device > FortiTokens**.

On the FortiAuthenticator

1. Go to **Authentication > User Management > Local Users**, and edit the user for which you want to deactivate the token.
2. Deselect **Token-based authentication**, and select **OK**.
   The token will be removed from the user's **Token** column. The user will also be removed from the token's User column, under **Authentication > User Management > FortiTokens**.

Considerations

The following information clarifies a few factors regarding different FortiToken deployments.

FortiToken authentication with no Internet

The following consideration is applicable to FortiOS 5.0+.

FortiTokens (excluding FortiToken-200CD) store their encryption seed files in the FortiGate or FortiAuthenticator unit they are assigned to. Their FortiTokens will continue to generate token codes. Therefore, FortiGate/FortiAuthenticator units can validate token codes and provide two-factor authentication even if they have lost access to the Internet.

Note that FortiToken Mobile needs access to FortiGuard for all management changes (such as token assignment to users). Once assigned, these tokens will work even if the FortiGate/FortiAuthenticator has no Internet access. However, FortiToken-200 user assignment without Internet access *is* possible.

FortiToken seed files

Both FortiToken Mobile and physical FortiTokens can only be registered to a single FortiGate or FortiAuthenticator unit. However, FortiToken-200CD seed files are stored on the CD, which means these tokens can be registered on multiple FortiGates and/or FortiAuthenticators, but *not* simultaneously.

HA clustering with FortiToken

In the case of setting up a High Availability (HA) cluster with multiple FortiGate/FortiAuthenticator units, you must register and apply your FortiToken licenses to the primary FortiGate unit. This can be done either before configuring the unit for HA operation, or after. After HA is configured, all tokens are replicated across cluster members. Because of this, you only need one FortiToken license per HA cluster. This is applicable for both FortiGate and FortiAuthenticator units.

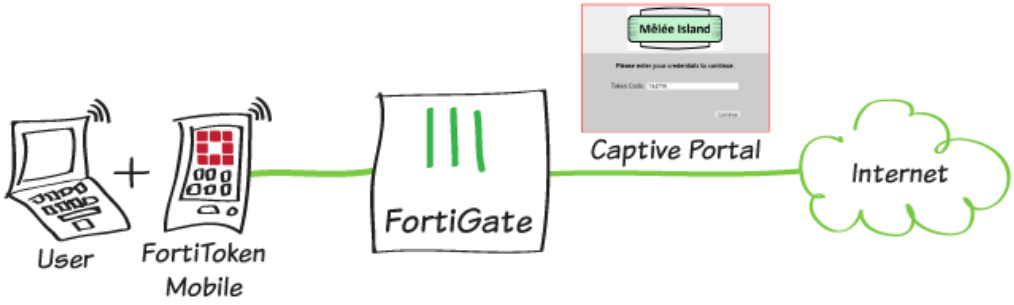
To learn more about HA clustering, see the FortiOS High Availability guide.

Configuration examples

The following section showcases a few FortiToken configuration examples, including:

- Example - Two-factor authentication with captive portal
- Example - IPsec VPN two-factor authentication with FortiToken-200
- Example - Captive portal WiFi access with FortiToken-200
- Example - FortiToken two-factor authentication with RADIUS on a FortiAuthenticator
- Example - Third-party token activation with Google

Example - Two-factor authentication with captive portal



In this scenario, you will set up a FortiGate to require users on an internal network to use two-factor authentication with FortiToken Mobile through a captive portal to access the Internet.

The captive portal will be added to the FortiGate's internal interface and you will customize the portal by changing the login page appearance and adding a new image.

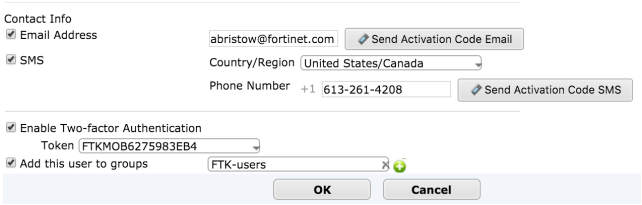
This scenario assumes that you have already added an Internet access policy, that you have added FortiToken Mobile to the FortiGate, and the **elainemarley** user is a member of the FortiToken user group named **FTK-users**.

1. Enabling FortiToken for elainemarley

Go to **User & Device > User Definition** and edit **elainemarley**.

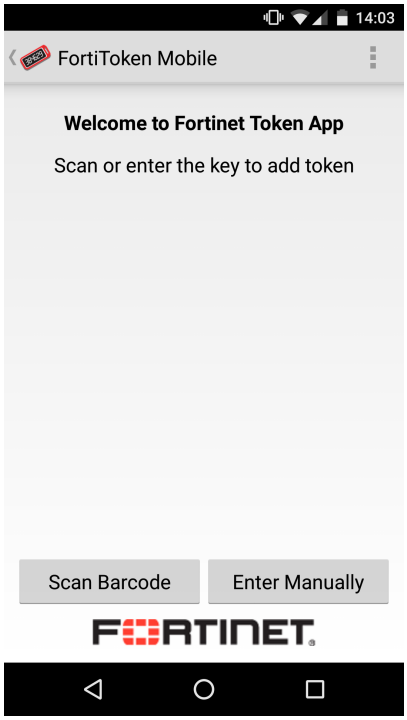
Select **Enable Two-factor Authentication** and select the FortiToken Mobile from the dropdown menu.

Under **Contact Info**, enable **Email Address** or **SMS**, enter elainemarley's contact information, and select **Send Activation Code Email** or **Send Activation Code SMS**. The internal network user will receive the activation code by the method specified.

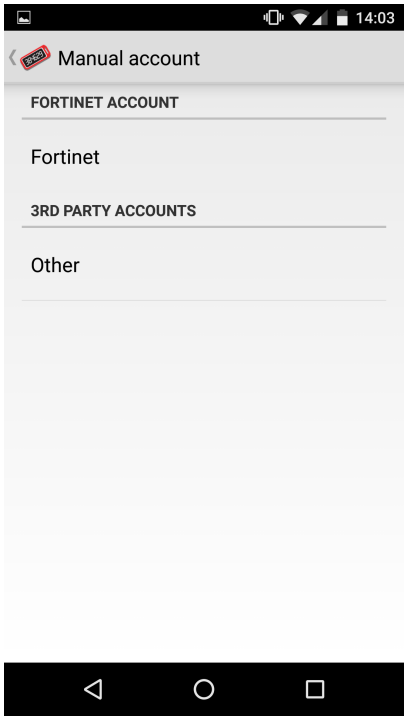


2. Adding a user account to FortiToken Mobile

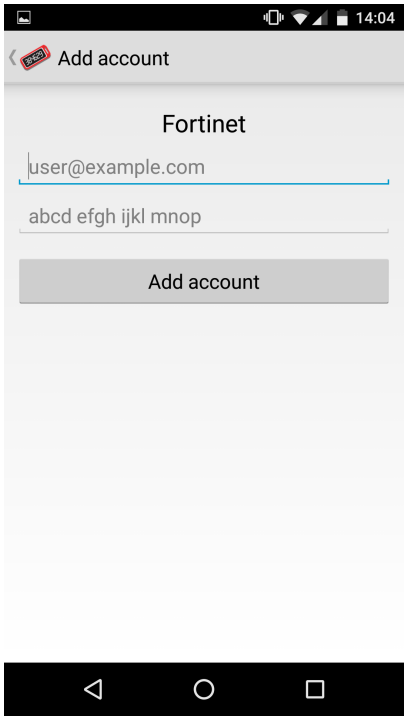
Open the FortiToken Mobile application and go to **Add account > Enter Manually > Fortinet**.



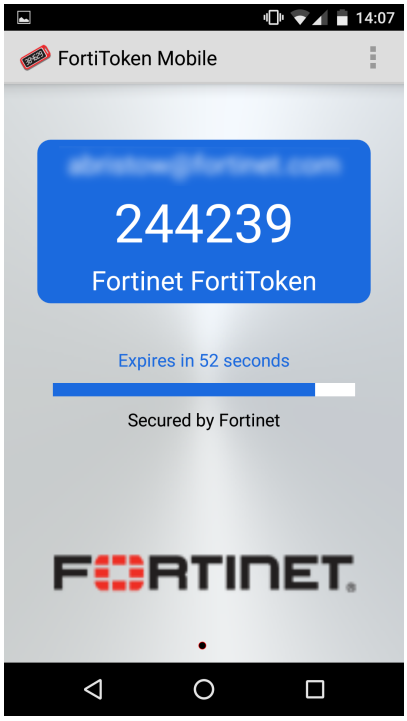
Use the **Scan Barcode** option to scan the attached QR code if you received your activation code by email instead of SMS.



Enter your email address, enter the activation code you received, and select **Add account**.



The token will activate and start generating codes.



3. Editing the internal interface

Go to **Network > Interfaces** and edit the internal interface.

Under **Admission Control**, set **Security Mode** to **Captive Portal**.

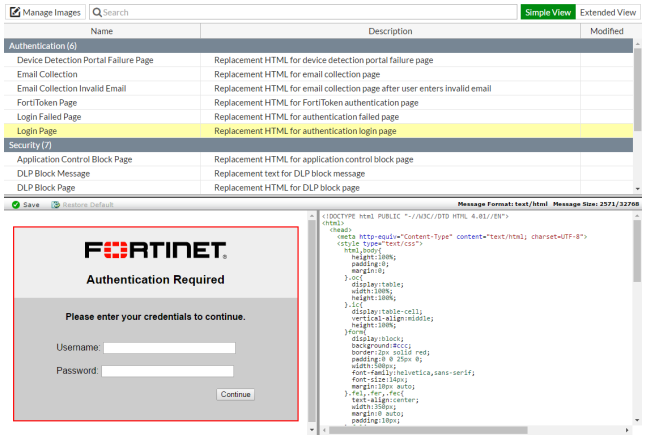
Set **Authentication Portal** to **Local**, and set **User Groups** to **FTK-users**.

4. Customizing the captive portal login page

Go to **System > Replacement Messages**. Under **Authentication**, select **Login Page**.

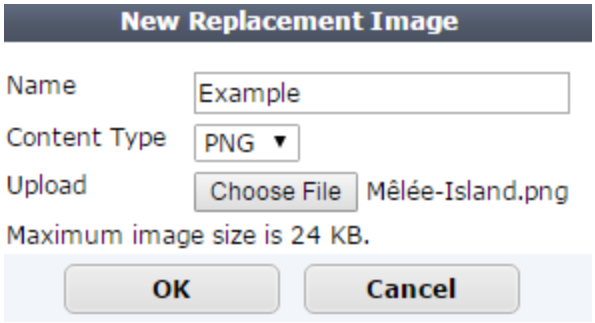
Two panels will open showing the login page that users will see when attempting to browse the Internet, and the HTML format.

You can customize the login page, such as border color and thickness, using the HTML panel. When finished, select **Save**, then select **Manage Images > Create New**.



Enter a name for the new replacement image, select a **Content Type** (select from **GIF**, **JPEG**, **TIFF**, or **PNG**), and upload an image file of your choice (in the example, *Mêlée-Island.png*).

Note that your image must be 24 KB or less.

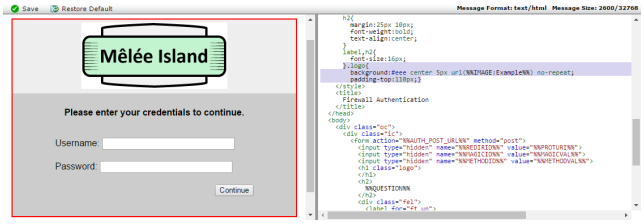


In the HTML panel for **Login Page**, scroll down to the logo, and configure the HTML as follows:

```
}.logo{
   background:#eee center 5px url(%%IMAGE:Example%%) no-repeat;
   padding-top:110px;}
```

Make any other changes you wish.

The new logo will replace the old image, as shown here.

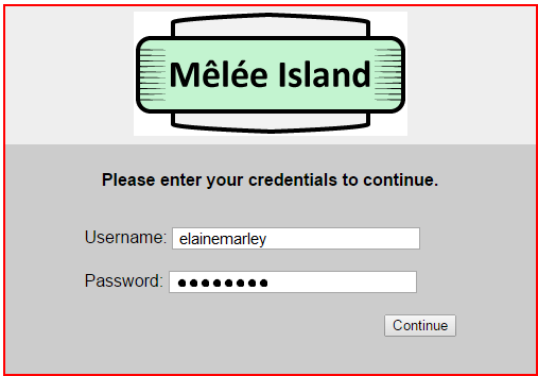


Under **Authentication**, select **FortiToken Page** and make the same customization changes made for the login page.

5. Results

Internal network users will be redirected to the captive portal login page when attempting to browse the Internet.

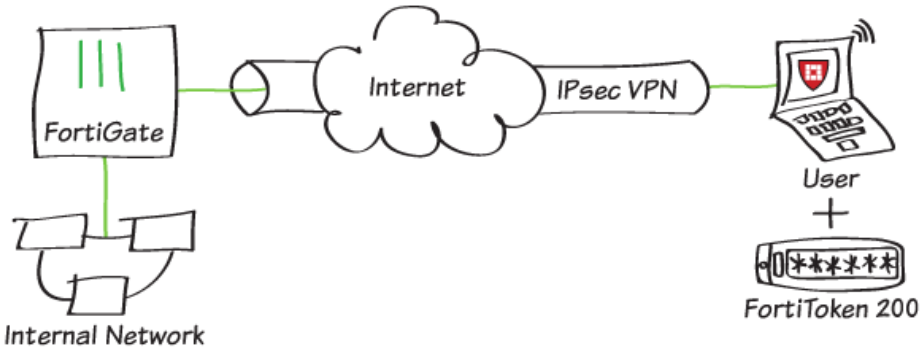
Enter **elainemarley**'s user credentials. You will then be prompted to enter a **FortiToken Code**. Enter the code and select **Continue**.



The user is now successfully authenticated and has access to the Internet.

To verify the **elainemarley**'s connection, go to **Monitor > FortiClient Monitor**.

Example - IPsec VPN two-factor authentication with FortiToken-200



In this scenario, you will configure two-factor authentication using a FortiToken-200 for IPsec VPN connections.

This configuration assumes that you have already created a user (*elainemarley*) and a user group (*FTK-users*). You will add a FortiToken-200 to the FortiGate, assign the token to the user, and add the user to the group. You will then use the Wizard to create an IPsec VPN tunnel that allows FortiToken-200 users to securely access an internal network and the Internet. You will test the setup by having the user access the VPN from a remote device, using FortiClient.

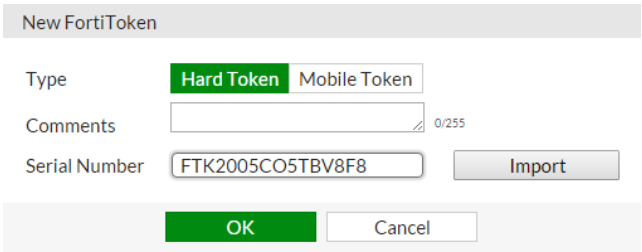
You can view a video of this configuration here.

1. Adding the FortiToken

Go to **User & Device > FortiTokens** and create a new FortiToken.

Set **Type** to **Hard Token** and enter the FortiToken's **Serial Number** into the field provided.

Note that the serial number, located on the back of the FortiToken device, is case sensitive and must not be in use elsewhere.

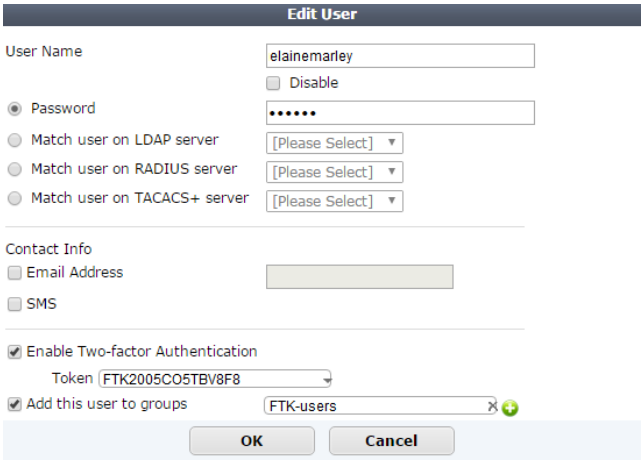


2. Editing the user and assigning the FortiToken

Go to **User & Device > User Definition** and edit **elainemarley**.

Select **Enable Two-factor Authentication** and select the token.

Select **Add this user to groups** and add the user to **FTK-users**.

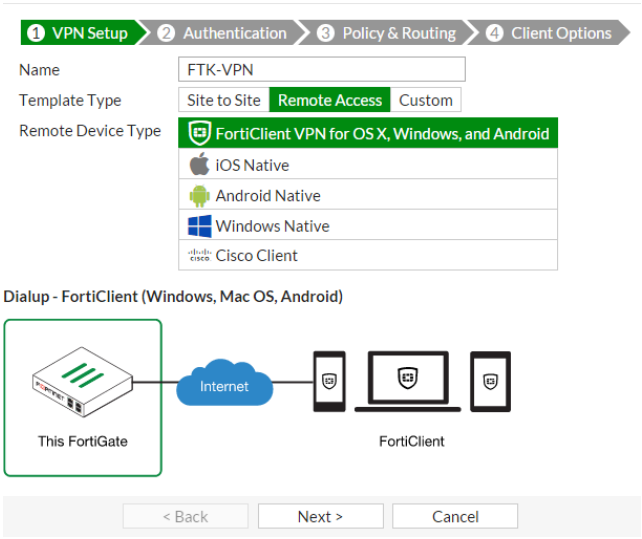


3. Configuring the IPsec VPN using the IPsec VPN Wizard

Go to **VPN > IPSec Wizard** and create a new IPsec VPN tunnel.

Name the VPN connection (in the example, *FTK-VPN*).

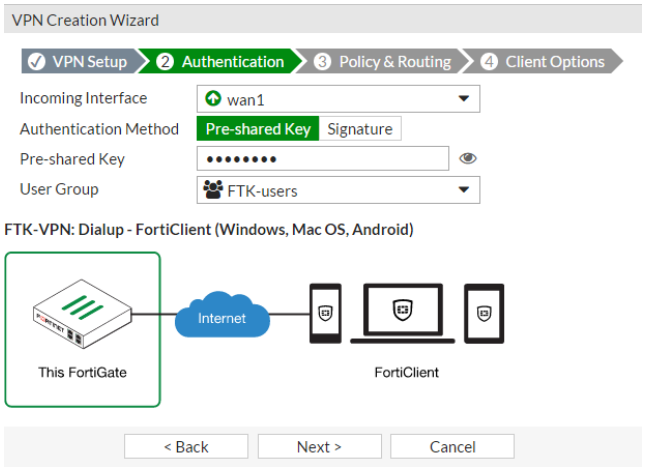
Select the **Remote Access** template, set **Remote Device Type** to **FortiClient VPN for OS X, Windows, and Android**, and select **Next**.



Set the **Incoming Interface** to the Internet-facing interface (**wan1**).

Set **Authentication Method** to **Pre-shared Key** and enter a pre-shared key.

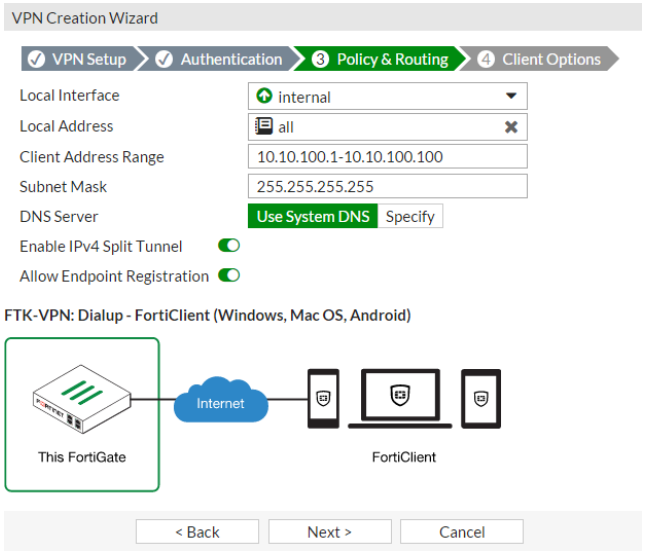
Select the user group created earlier (**FTK-users**) and select **Next**.



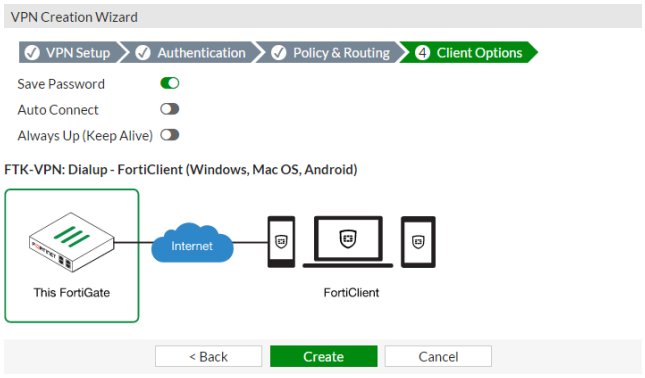
Set **Local Interface** to the internal interface and set **Local Address** to **all**.

Enter an IP address range for VPN users in the **Client Address Range** field. [tippy title="*" class="myclass" showheader="false" width="auto" height="auto"]Make sure no other interfaces on the FortiGate are using the same address range.[/tippy] A **Subnet Mask** should already be set.

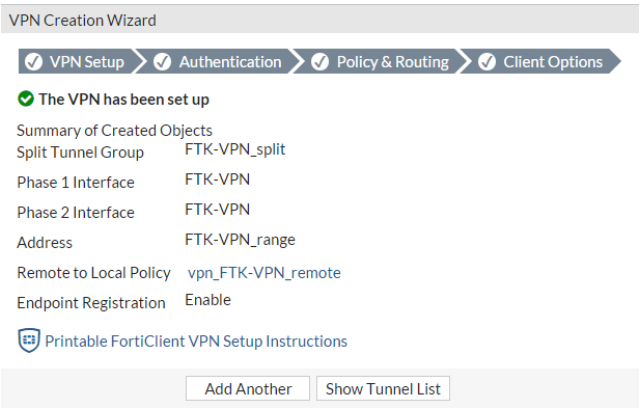
Select **Next**.



Configure additional **Client Options** and select **Create**.



A summary page will appear showing the VPN's configuration.



4. Connecting to the IPsec VPN

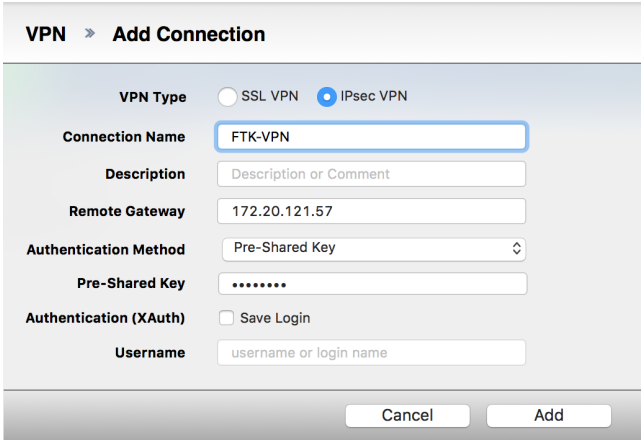
On your remote device, open the FortiClient application, go to **Remote Access**, and add a new connection.

Set **VPN Type** to **IPsec VPN**, and enter a **Connection Name**.

Set **Remote Gateway** to the IP address of the FortiGate, set **Authentication Method** to **Pre-Shared Key**, and enter a **Pre-Shared Key**.

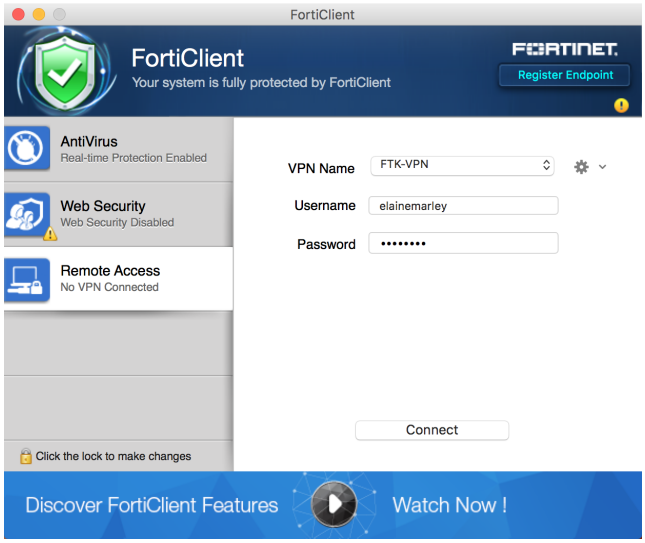
The key must match the same key entered in the wizard on the FortiGate earlier.

When finished, select **Add**.

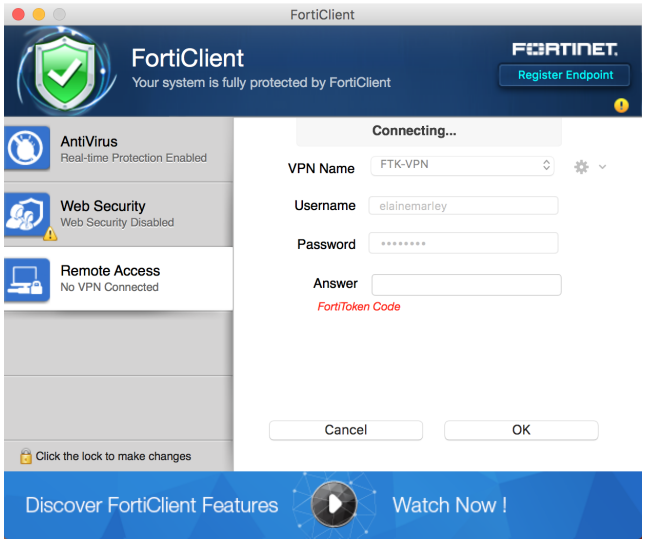


5. Results

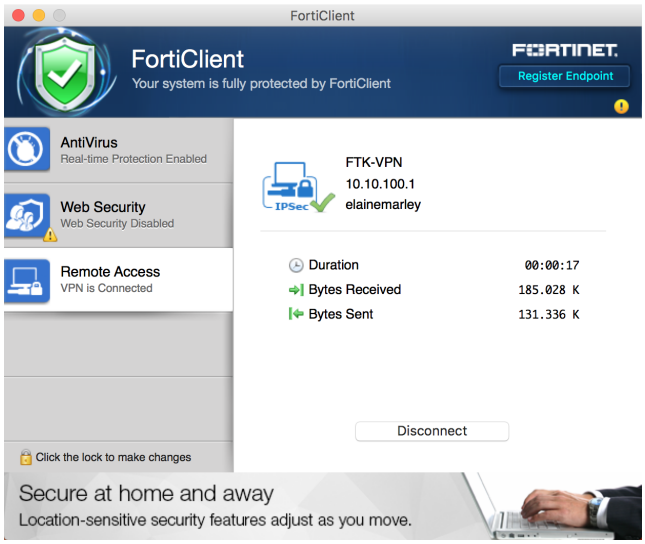
Go to **Remote Access** and attempt to log into the VPN as **elainemarley**.



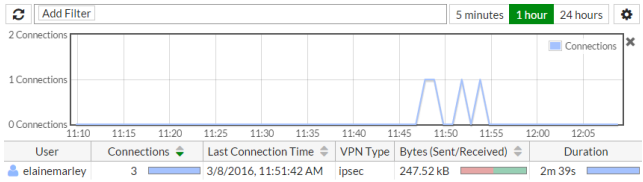
You will then be prompted to enter a **FortiToken Code**. Enter the code and select **OK**.



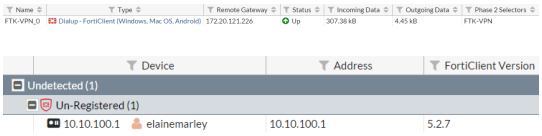
The user is now successfully connected to the IPsec VPN **FTK-VPN**.



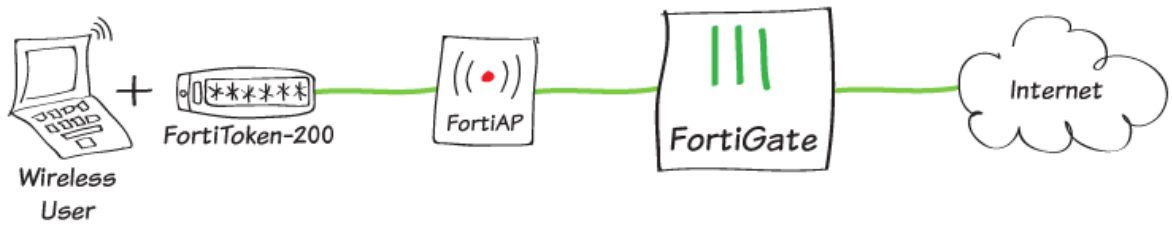
To verify the user's connection, go to **FortiView > VPN**.



You can also go to **Monitor > IPsec Monitor** to view the tunnel's status, and **Monitor > FortiClient Monitor** to view the user and device.



Example - Captive portal WiFi access with FortiToken-200



In this scenario, you will enforce two-factor authentication for WiFi users who have FortiToken-200 devices through a captive portal. FortiToken-200 users who attempt to browse the Internet will be redirected to the captive portal login page and asked to enter their username, password, and six-digit authentication code.

This scenario assumes that you already have a FortiAP unit connected and authorized to the FortiGate, and that the SSID has been set up and configured to use captive portal. To see how to set up a wireless network through a captive portal, see our online cookbook configuration: Captive portal WiFi access control.

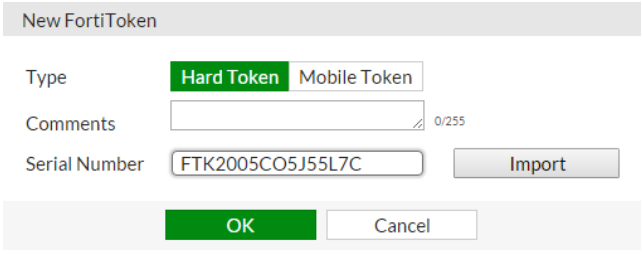
This configuration is designed for a FortiToken-200 physical key generator. See step 2 for information about using FortiToken Mobile.

You can view a video of this configuration here.

1. Adding the FortiToken

Go to **User & Device > FortiTokens** and create a new FortiToken.

Set **Type** to **Hard Token** and enter the **Serial Number** into the field provided and select **OK**.

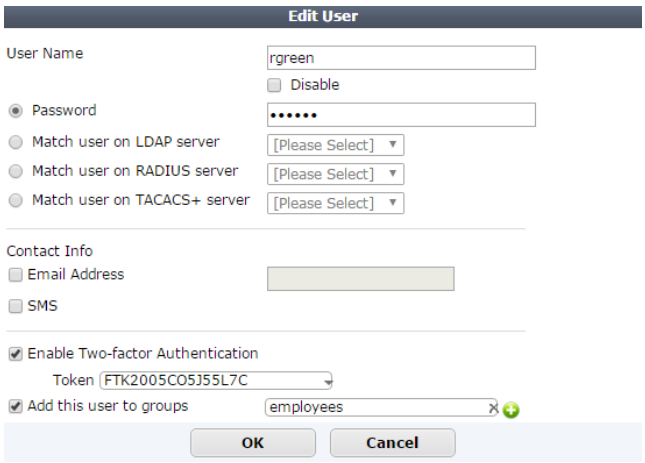


2. Editing the user and assigning the FortiToken

Go to **User & Device > User Definition** and edit the user (*rgreen*).

Select **Enable Two-factor Authentication** and select the token created earlier.

Select **Add this user to groups** and add the user to the captive portal user group (*employees*).

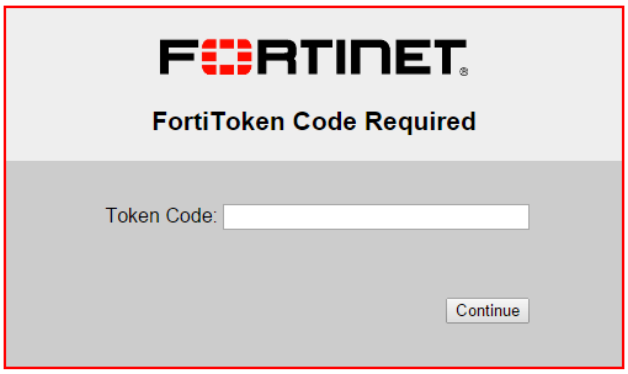


This recipe is designed for a FortiToken-200 physical key generator. If the user has FortiToken Mobile, the user's contact information *must* be included so that the FortiToken code can be sent to the user via Email or SMS.

3. Results

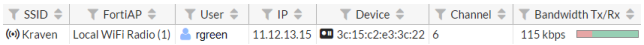
When a user attempts to browse the Internet, they will be redirected to the captive portal login screen.

Members of the FortiToken group must enter their **Username** and **Password**, but will then be redirected to a screen requiring the user to enter their **Token Code**.[tippy title="*" class="myclass" showheader="false" width="auto" height="auto"]Retrieve the code by pressing the button on the FortiToken device.[/tippy]

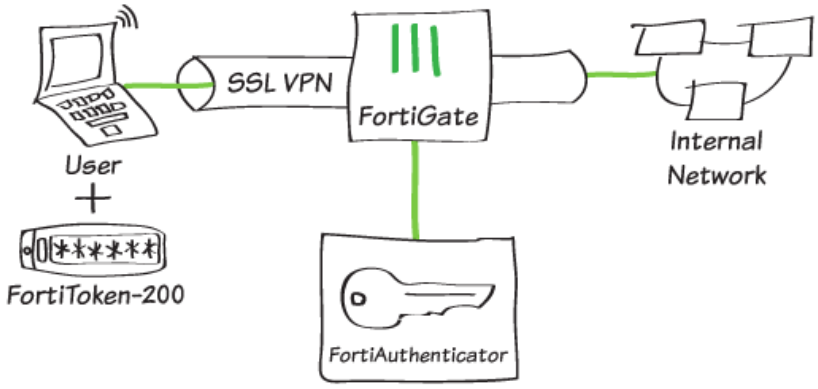


Once the code is successfully entered, the user will be redirected to the URL originally requested.

On the FortiGate, go to **Monitor > WiFi Client Monitor** to verify that the user is authenticated.



Example - FortiToken two-factor authentication with RADIUS on a FortiAuthenticator



In this scenario, you will set up FortiAuthenticator to function as a RADIUS server to allow SSL VPN users to authenticate with a FortiToken-200.

This scenario assumes that you have already added the FortiToken, assigned it to the user, and added the user to a group for FortiToken users on the FortiAuthenticator.

You will configure a user, FortiToken-200, the RADIUS client on the FortiAuthenticator, and the FortiGate to use the FortiAuthenticator as a RADIUS server. You will then create the SSL VPN tunnel.

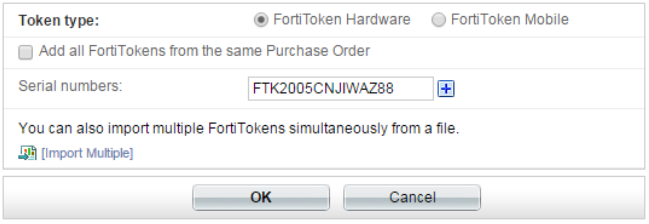
You can view a video of this configuration here.

1. Adding the FortiToken to FortiAuthenticator

On the FortiAuthenticator, go to **Authentication > User Management > FortiTokens**, and select **Create New**.

Make sure **Token type** is set to **FortiToken-200**, and enter the FortiToken's serial number into the field provided.

The serial number, located on the back of the FortiToken device, is case sensitive. Note that the token can only be registered to one device.

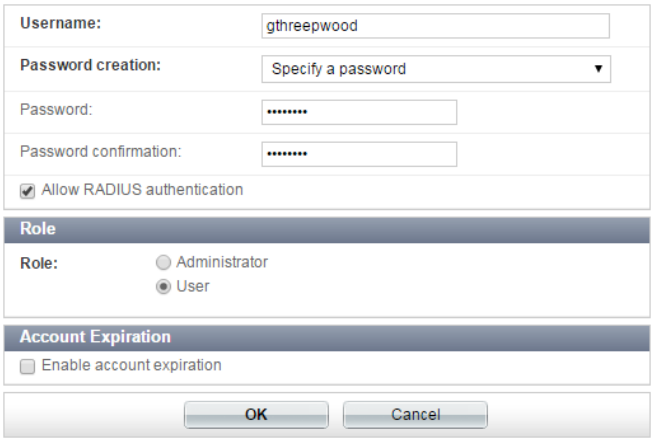


2. Adding the FortiToken user to FortiAuthenticator

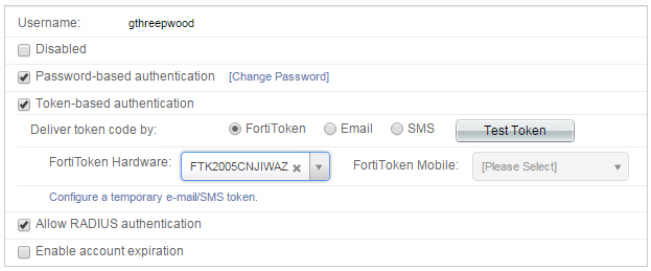
On the FortiAuthenticator, go to **Authentication > User Management > Local Users**, and select **Create New**.

Enter a **Username** (*gthreepwood*), enter and confirm a password, and make sure that **Allow RADIUS authentication** is enabled.

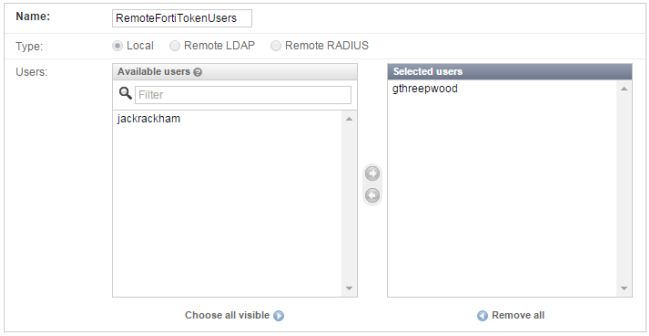
Select **OK** to access additional settings.



Enable **Token-based authentication**, select to deliver the token code by **FortiToken**, and select the FortiToken added earlier from the **FortiToken-200** dropdown menu.



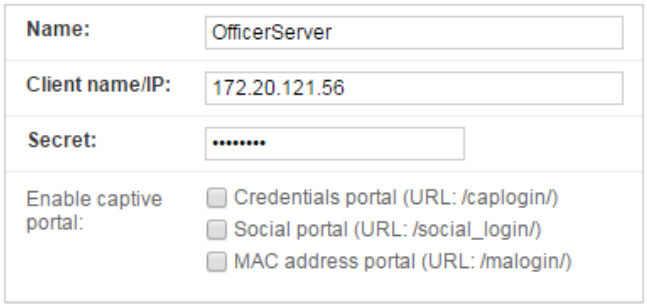
Next, go to **Authentication > User Management > User Groups**, create a user group (*RemoteFortiTokenUsers*), and add **gthreepwood** to the group.



3. Creating the RADIUS Client on FortiAuthenticator

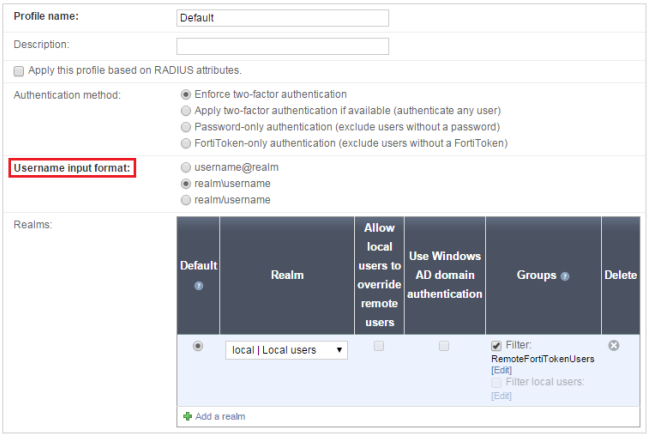
On the FortiAuthenticator, go to **Authentication > RADIUS Service > Clients**, and select **Create New**.

Enter a name (*OfficeServer*), set **Client name/IP** to the IP of the FortiGate, and set a **Secret**. The secret is a pre-shared, secure password that the FortiGate will use to authenticate to the FortiAuthenticator.



Set **Authentication method** to **Enforce two-factor authentication**, set **Realms** to **local | Local users**, and add **RemoteFortiTokenUsers** to the **Groups** filter.

Note the **Username input format**. This is the format that the user must use to enter their username in the web portal.

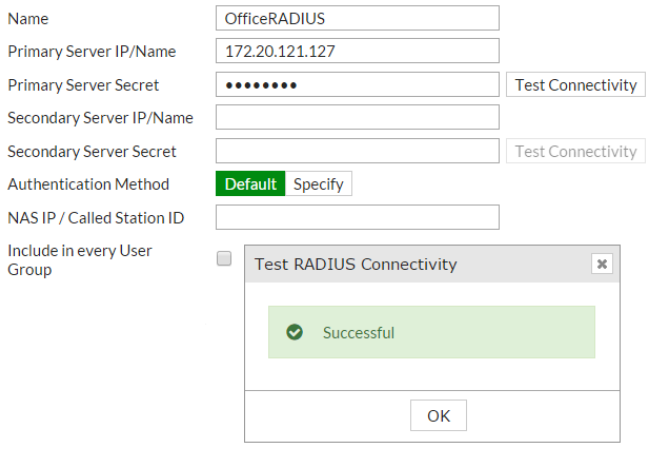


4. Connecting the FortiGate to the RADIUS Server

On the FortiGate, go to **User & Device > RADIUS Servers**, and select **Create New**.

Enter a **Name** (*OfficeRADIUS*), set **Primary Server IP/Name** to the IP of the FortiAuthenticator, and enter the **Secret** created before.

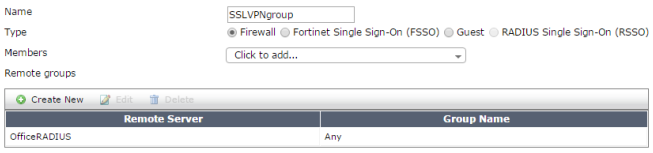
Test the connectivity and enter the credentials for **gthreepwood**. The test should come back with a successful connection.
The FortiGate can now log into the RADIUS client added earlier to the FortiAuthenticator.



On the FortiGate, go to **User & Device > User Groups**, and select **Create New**.

Enter a **Name** (*SSLVPNGroup*), and under **Remote groups**, select **Create New**.

Select **OfficeRADIUS** under the **Remote Server** dropdown menu.



5. Configuring the SSL VPN on FortiGate

On the FortiGate, go to **VPN > SSL-VPN Portals**, and edit the **full-access** portal.

Disable **Split Tunneling**.

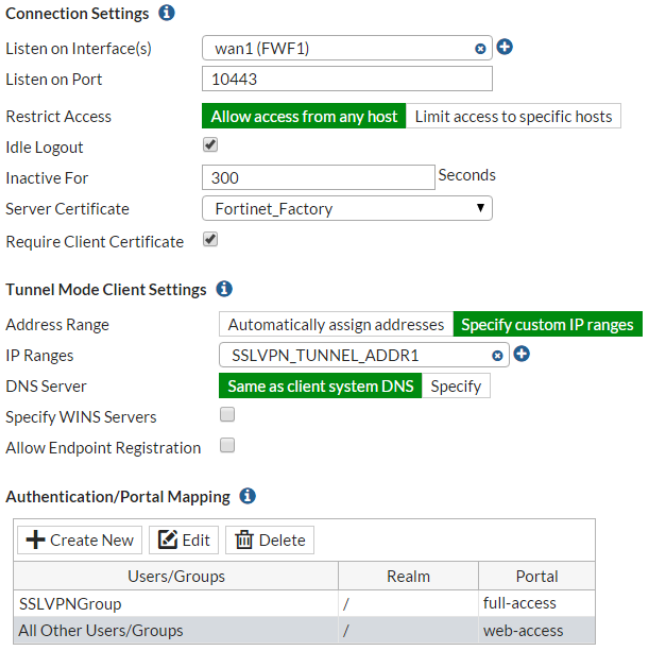
Go to **VPN > SSL-VPN Settings**.

Under **Connection Settings** set **Listen on Port** to **10443**.

Under **Tunnel Mode Client Settings**, select **Specify custom IP ranges** and set it to **SSLVPN_TUNNEL_ADDR1**.

Under **Authentication/Portal Mapping**, select **Create New**.

Assign the **SSLVPNGroup** user group to the **full-access** portal, and assign **All Other Users/Groups** to **web-access** — this will grant all other users access to the web portal *only*.

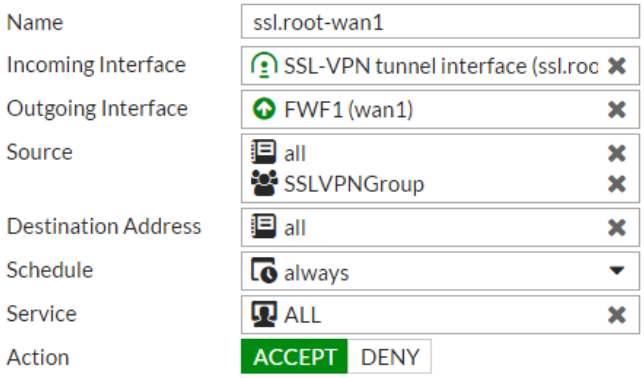


Go to **Policy & Objects > IPv4 Policy** and create a new SSL-VPN policy.

Set **Incoming Interface** to the **SSL-VPN tunnel interface** and set **Outgoing Interface** to the Internet-facing interface.

Set **Source** to the **SSLVPNGroup** user group and set **Destination Address** to **all**.

Set **Schedule** to **always**, **Service** to **ALL**, and enable **NAT**.

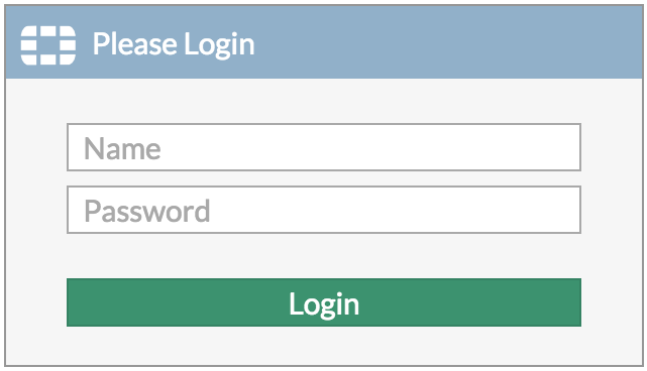


6. Results

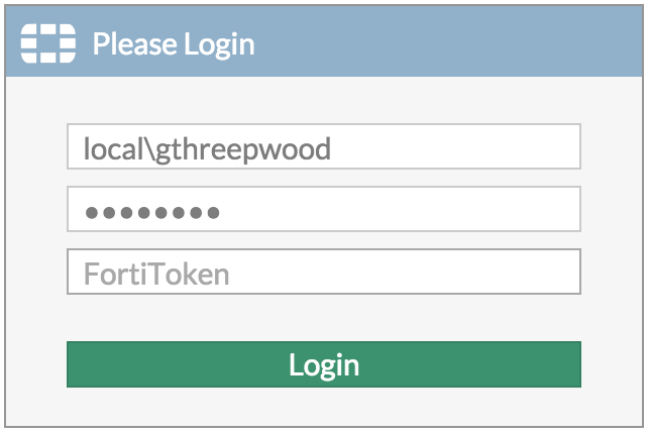
From a remote device, open a web browser and navigate to the SSL VPN web portal (*https://FortiGate-IP:10443*).

Enter **gthreepwood**'s credentials and select **Login**.

Note that the username has to be entered in the format '*realm\username*', as per the client configuration on the FortiAuthenticator (in this example, *local\gthreepwood*).

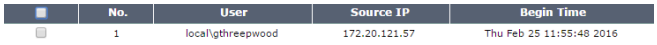


The user will then be prompted to enter their FortiToken code.

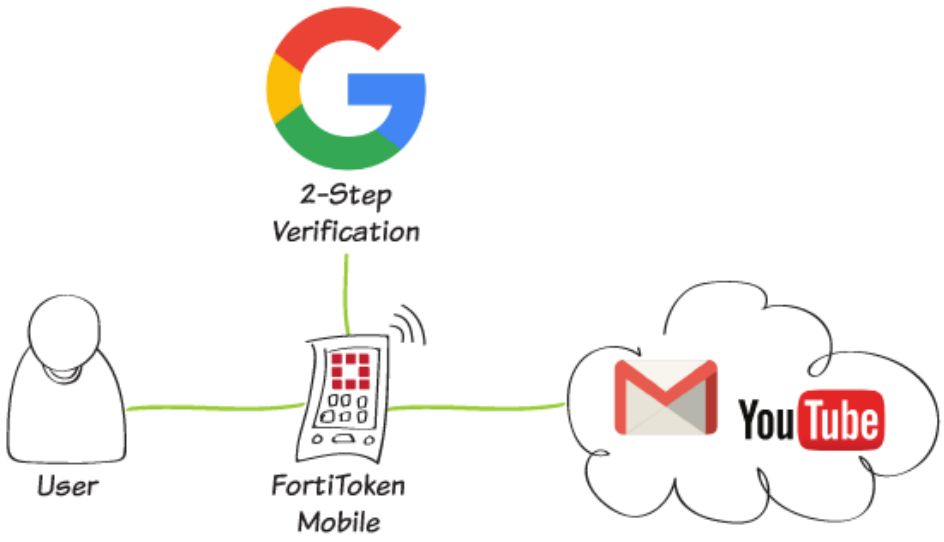


Once the code is successfully entered, **gthreepwood** will successfully log into the SSL VPN Portal.

On the FortiGate, go to **Monitor > SSL-VPN Monitor** to confirm the user's connection.



Example - Third-party token activation with Google



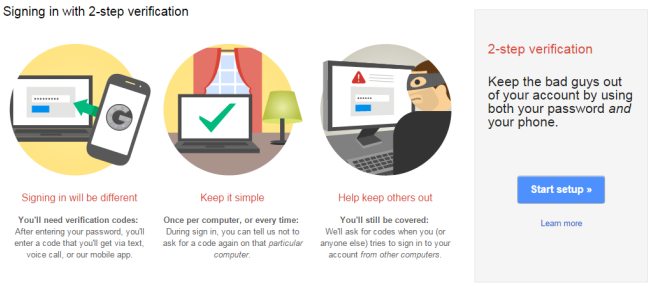
In this scenario, you will enable Google's "2-Step Verification" and add the Google token to your FortiToken Mobile for third-party two-factor authentication.

1. Configure Google 2-Step Verification on the browser

Open a browser and log in to your Google account at https://myaccount.google.com.

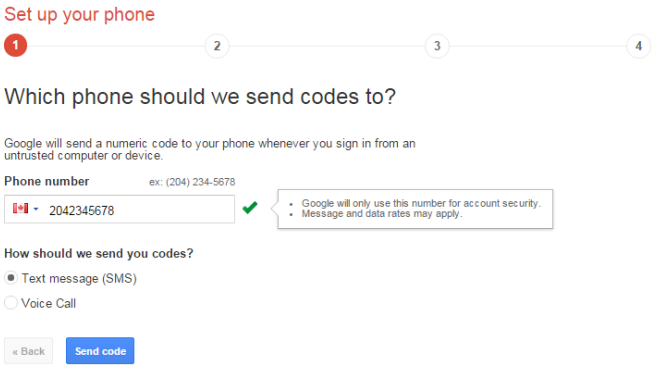
Select **Sign-in & security**.

Under **Signing in to Google**, select **2-Step Verification** (re-enter your password if necessary) and select **Start setup**.

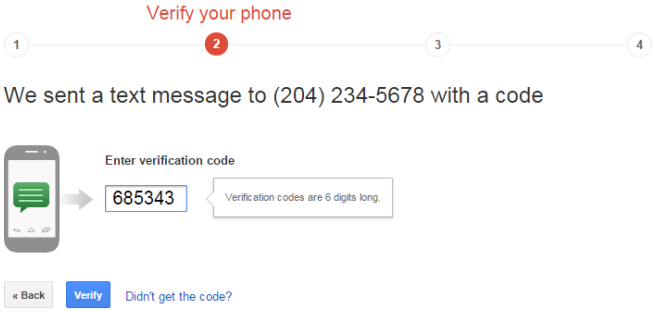


Enter your phone number, select to have your code sent to you by **Text message (SMS)**, and select **Send code**.

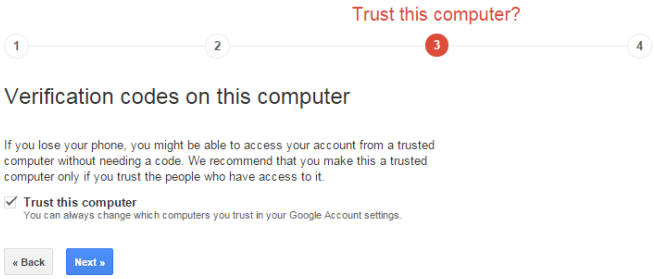
Shortly afterwards you will receive an SMS text message with a 6-digit verification code.



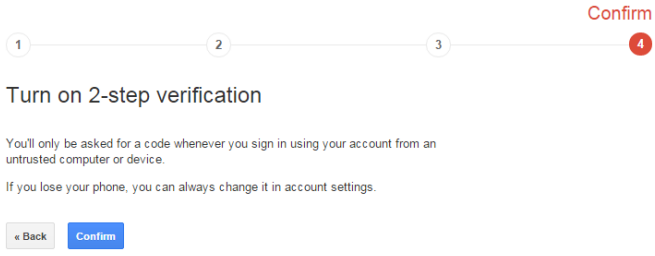
Enter the verification code in your browser and select **Verify**.



Elect to **Trust this computer** and select **Next**.

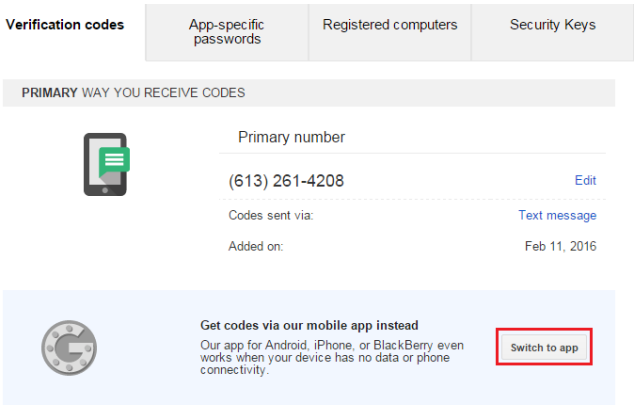


To confirm the 2-Step Verification set up, select **Confirm**.

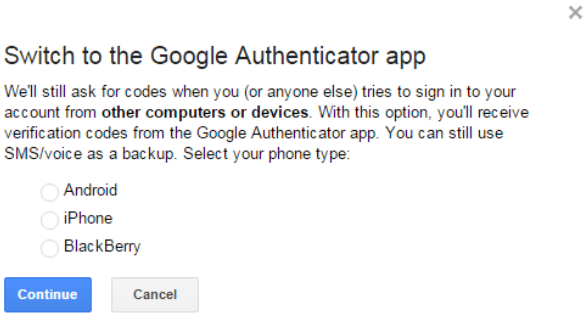


You will be redirected to your Google **2-Step Verification** page.

Select **Switch to app**.



Select your phone type (**Android**, **iPhone**, or **Blackberry**) and select **Continue**.



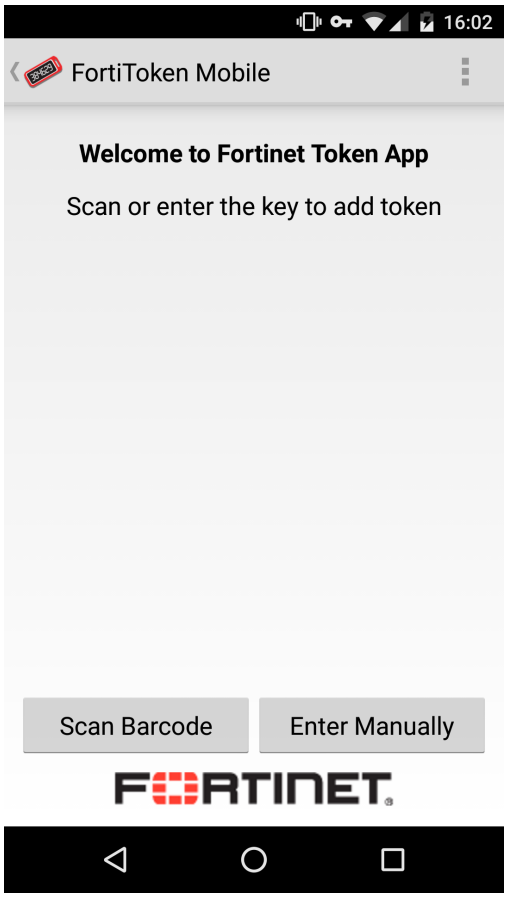
2. Add Google 2-Step Verification to FortiToken

Open FortiToken Mobile on your phone and enter your 4-digit PIN.

Select **Add account**.

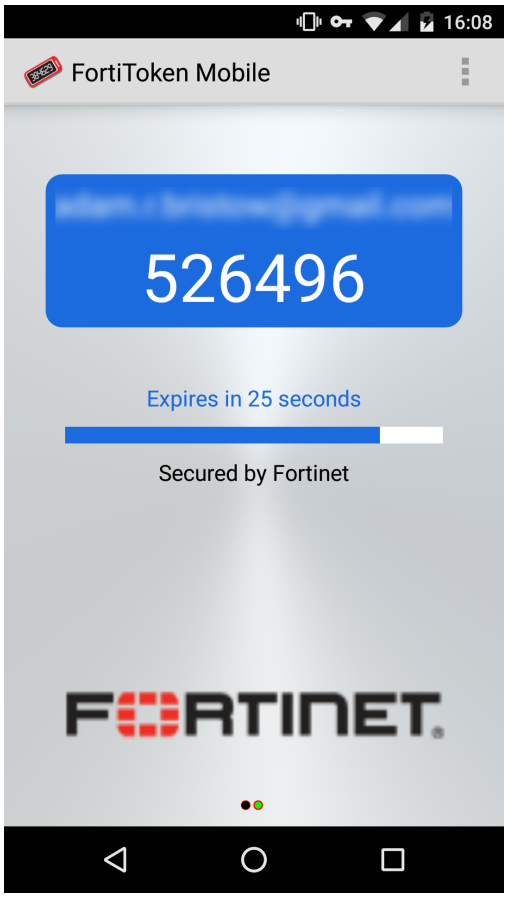
Select **Scan Barcode** or **Enter Manually**.

If you choose to **Enter Manually**, make sure to select **3rd Party Accounts > Other**. The account name will be the email address of the user.

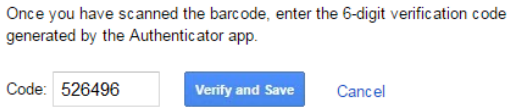


Scan the barcode presented in the Google Authenticator set up window, or select **Can't scan the barcode?** to view and enter the secret key into FortiToken Mobile manually.

FortiToken Mobile will begin producing Google authentication codes.



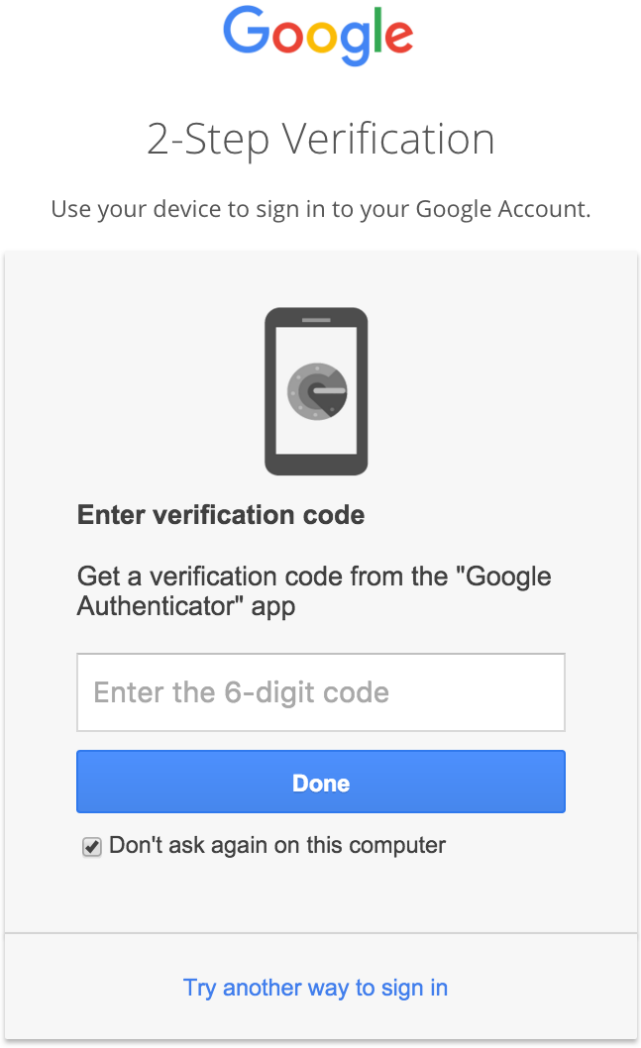
In the Google Authenticator set up window, enter the 6-digit code presented in FortiToken Mobile and select **Verify and Save**.



3. Results

When attempting to log in to a Google account (Gmail or YouTube for example), the user will be prompted to enter their verification code.

Enter the code displayed in FortiToken Mobile and select **Done**.



Reference

The following section provides additional reference information for FortiToken-200, FortiToken-200CD, and FortiToken Mobile.

The FortiToken-200CD uses the serial number prefix **FTK211** on the back side of the physical token in order to distinguish it from the standard FortiToken-200, which uses the serial number prefix **FTK200**.

FortiToken Mobile uses the serial letter prefix **FTKMOB**.

FortiToken platform scalability

The following table shows the maximum number of FortiTokens that can be assigned to certain FortiGate and FortiAuthenticator models. Note that FortiToken is also supported on specific FortiWiFi models.

All data for this table was taken from the following Product Matrix datasheet.

FortiGate Models	Max. FortiTokens
30D / 30E	20
50E / 60D / 60E / 70D / 80D / 90 series	100
100D / 140D / 200D / 240D / 280D POE / 300D / 400D / 500D / 600D / 800C / 900D	1,000
1000D / 1200D / 1500D / 3000D / 3100D / 3200D / 3700D / 3810D / 3815D / 5001D VMware / Xen / AWS / AWS on Demand / KVN / Hyper V	5,000

FortiAuthenticator Models	Max. FortiTokens
200D	500
400C	2,000
1000D	10,000
3000D	40,000
VM BASE to VM-100000-UG	200 to 200,000+

Drift adjustment

If a user experiences clock drift, it may be the result of incorrect device time settings. If so, make sure that the mobile device clock is accurate by confirming the network time and correct timezone.

If the device clock is set correctly, the issue may be the result of the FortiAuthenticator unit and FortiTokens being initialized prior to setting an NTP server -- this will result in a time difference that is too large to correct with the synchronize function. To avoid this, selected tokens can be manually drift adjusted.

The following procedure is intended to be used only in special cases where some FortiTokens are severely out-of-sync, for example, when a token is switched from manual configuration to NTP control. Under normal circumstances, this is not required.
Only activated FortiTokens can be adjusted.

To perform time drift adjustment on a FortiToken:

1. In a browser, go to `https://<FortiAuthenticator-IP-Address>/admin/fac_auth/fortitokendrift/`.
2. Select the FortiToken to adjust and select **Adjust Drift**.
3. Enter the required **Time adjustment** in minutes.
   Include a minus sign (**-**) for a negative value, but don't use a plus sign (**+**) for a positive value.
4. Select **OK** to adjust the token drift by the specified time.

Diagnosing FortiToken on the FortiGate

The following diagnose debug command will show a list of your FortiTokens, their drift, and status:

```
diag fortitoken info
```

```
FORTITOKEN       DRIFT  STATUS
FTK200XXXXXXXXXX 0      new
FTK211XXXXXXXXXX 0      new
FTKMOBXXXXXXXXXX 0      new

Total activated token: 0
Total global activated token: 0

Token server status: reachable
```

Status outputs:

- `new`

  Newly added to the FortiGate and not assigned to a user.

- `active`

  Assigned to a user. This output is for FortiToken-200 and 200 CD only.

- `provisioned`

User has activated their token and is assigned to them. This output is for FortiToken Mobile only.

- `provision timeout`

  The administrator has set the token to the user, but the user has not activated the token within the timeout period. The token must be re-provisioned to the user.

- `token already activated, and seed won't be returned`

  FortiToken-200 has been added, removed, and re-added to the FortiGate. FortiToken-200 can only be transferred from one FortiGate or FortiAuthenticator device to another by contacting customer support.

- `activation error (token not exist in FortiGuard)`

  FortiToken-200 CD has been imported with the activation CD, but there is no contact to the FortiGuard server. Contact customer support.

When contacting customer support, you must provide the FortiToken serial number, as well as the FortiGate or FortiAuthenticator serial number to which the token is assigned.

FortiToken provisioning with FortiAuthenticator REST API

The FortiAuthenticator API can be accessed (without additional cost or licensing) so that third-party user provisioning systems can confirm which FortiTokens are available to be provisioned to a user.

For the API to be accessible, a user must be granted administrator privileges so that they can log in. To view the FortiToken resource, cURL is being used to make the requests. For more information on how to do this, see the FortiAuthenticator REST API Solution Guide.

Accessing the REST API

To access the REST API resource, you must browse to the following URL:

https://[server_name]/api/[api_version]/[resource]/

- **server_name**: Name or IP address of the FortiAuthenticator.
- **api_version**: API version to be used (currently **v1**).
- **resource**: Resource of part of config to be viewed.

  For the purposes of accessing FortiToken information, the resource is **/fortitokens/**.

To view a list of all the available resource end-points, send a request to https://[server_name]/api/v1/?format=xml.

FortiToken resource - /fortitokens/

URL: https://[server_name]/api/[api_version]/fortitokens/

In this FortiAuthenticator GUI, this resource corresponds to **Authentication > User Management > FortiTokens**. As mentioned earlier, this API is used by third-party user provisioning systems to confirm which FortiTokens are available to be provisioned to a user.

Supported Fields

Field	Display Name	Type	Required	Other Restriction
serial	Serial number	string	No	
type	Type	string	No	Either `ftk` or `ftm`.
status	Status	string	No	Either `new`, `available`, `pending`, or `assigned`.

Allowed methods

Type	Allowed Methods	Action
List	GET	Get all FortiTokens.

Allowed filters

Field	Lookup Expressions	Values
serial	exact, iexact	
type	exact, iexact	Either `ftk` or `ftm`.
status	exact, iexact	Either `new`, `available`, `pending`, or `assigned`.

View all tokens

JSON Query

- JSON specified via GET

```
curl -k -v -u "admin:zeyDZXmP6GbKcerqdWWEYNTnH2TaOCz5HTp2dAVS"
    https://192.168.0.122/api/v1/fortitokens/?format=json
```

Response

```
< HTTP/1.1 200 OK
< Date: Mon, 09 Jun 2014 18:17:42 GMT
< Server: Apache
< Vary: Accept,Accept-Language,Cookie
< X-Frame-Options: SAMEORIGIN
< Content-Language: en
< Cache-Control: no-cache
< Transfer-Encoding: chunked
< Content-Type: application/json
<
* Connection #0 to host 192.168.0.122 left intact
* Closing connection #0
```

```
{"meta": {"limit": 20, "next": null, "offset": 0, "previous": null, "total_count": 2},
   "objects": [{"resource_uri": "/api/v1/fortitokens/1/", "serial": "FTKMOB44142CCBF3",
   "status": "available", "type": "ftm"}, {"resource_uri": "/api/v1/fortitokens/2/",
   "serial": "FTKMOB4471BB94D1", "status": "available", "type": "ftm"}]}
```


View subset of tokens using filters

This example shows how to obtain a list of specific tokens, for example the first available FortiToken Mobile (FTM) token.

JSON Query

- JSON specified via GET

```
curl -k -v -u "admin:zeyDZXmP6GbKcerqdWWEYNTnH2TaOCz5HTp2dAVS" -H 'Accept:
application/json'
"https://192.168.0.122/api/v1/fortitokens/?format=json&type=ftm&status=available&limit
=1"
```

The URL requires additional quoting in this case otherwise the Unix CLI treats the "&" as an instruction to place the cURL command into the background.

Response

```
< HTTP/1.1 200 OK
< Date: Mon, 09 Jun 2014 18:17:42 GMT
< Server: Apache
< Vary: Accept,Accept-Language,Cookie
< X-Frame-Options: SAMEORIGIN
< Content-Language: en
< Cache-Control: no-cache
< Transfer-Encoding: chunked
< Content-Type: application/json
<
* Connection #0 to host 192.168.0.122 left intact
* Closing connection #0
{"meta": {"limit": 1, "next":
   "/api/v1/fortitokens/?status=available&type=ftm&offset=1&limit=1&format=json",
   "offset": 0, "previous": null, "total_count": 2}, "objects": [{"resource_uri":
   "/api/v1/fortitokens/1/", "serial": "FTKMOB44142CCBF3", "status": "available", "type":
   "ftm"}]}
```

Authentication resource - /auth/

URL: https://[server_name]/api/[api_version]/auth/

The Authentication API is for validation of user credentials. Either the password, token, or both can be validated. This is useful for adding an additional factor authentication (e.g. token) to web portals where the first factor has already been locally validated (e.g. via LDAP, local DB, or a proprietary, unsupported authentication method).

To authenticate a user, you need to POST to https://[server_name]/api/v1/auth/ with the following key-value pair (in JSON format, but XML is also possible):

```
{"username": "<username>", "token_code": "<token_code>", "password":
   "<password>"}
```

The `token_code` and `password` fields are optional, i.e. you can validate the token only, or the password only. If both token and password are specified, the password will be validated first before the token code. Furthermore, if a user doesn't have two-factor authentication configured, validation for that user with any `token_code` will fail.

Supported fields

Field	Display Name	Type	Required	Other Restriction
username	Username	string	Yes	
password	Password	string	No	
token_ code	Security token code	string	No	Supported token authentication: FortiToken, email token, SMS token

Allowed methods

Type	Allowed Methods	Action
List	POST	Validate user's credentials

Response codes

In addition to the general response codes, a POST request to this resource can result in the following return codes:

Code	Response Content	Description
200 OK		User is successfully authenticated.
401 Unauthorized	User authentication failed	Credentials are incorrect.
401 Unauthorized	Account is disabled	User account is currently disabled.
401 Unauthorized	No token configured	User does not have token-based authentication configured.
401 Unauthorized	Token is out of sync	The security token requires synchronization.
404 Not Found	User does not exist	The given username does not exist in the system.

To see the general response codes, see the FortiAuthenticator REST API Solution Guide (Appendix A - API Response Codes).

Validate a user password

JSON Query

- JSON specified via Accept Header

```
curl -k -v -u "admin:zeyDZXmP6GbKcerqdWWEYNTnH2TaOCz5HTp2dAVS" -d '
   {"username":"testuser","password":"testpass"}' -H "Content-Type: application/json"
```

```
https://192.168.0.122/api/v1/auth/
```

Response

```
< HTTP/1.1 200 OK
< Date: Fri, 14 Sep 2012 15:38:57 GMT
< Server: Apache
< Vary: Cookie
< Set-Cookie: sessionid=6b17c5bbb86419a94f6979a05bd84139; httponly; Path=/
< Content-Length: 0
< Content-Type: text/html; charset=utf-8
```

Validate a users token code

JSON Query

- JSON specified via Content-Type Header

```
curl -k -v -u "admin:zeyDZXmP6GbKcerqdWWEYNTnH2TaOCz5HTp2dAVS" -d '
   {"username":"testuser","token_code":"893753"}' -H "Content-Type: application/json"
   https://192.168.0.122/api/v1/auth/
```

Response

```
< HTTP/1.1 200 OK
< Date: Fri, 14 Sep 2012 15:47:22 GMT
< Server: Apache
< Vary: Cookie
< Set-Cookie: sessionid=f15beeab159a4bf2d0402a05db40d6ae; httponly; Path=/
< Content-Length: 0
< Content-Type: text/html; charset=utf-8
```

Error states

Response (incorrect password)

```
HTTP/1.1 401 UNAUTHORIZED
Date: Thu, 13 Sep 2012 13:57:24 GMT
Server: Apache
Vary: Cookie
Set-Cookie: sessionid=abe8bac6fc50caf5eadf1e57f0c60e3e; httponly; Path=/
Content-Length: 26
Content-Type: text/html; charset=utf-8
```

Response (incorrect token code)

```
HTTP/1.1 401 UNAUTHORIZED
Date: Thu, 13 Sep 2012 13:55:18 GMT
Server: Apache
Vary: Cookie
Set-Cookie: sessionid=e95090804ee0e3b8903618138b38a5c8; httponly; Path=/
Content-Length: 26
Content-Type: text/html; charset=utf-8
```

Response (incorrect username)

```
HTTP/1.1 404 NOT FOUND
Date: Thu, 13 Sep 2012 13:58:54 GMT
Server: Apache
Vary: Cookie
Set-Cookie: sessionid=3b353061d9141567c02bb0d057b18284; httponly; Path=/
Content-Length: 19
Content-Type: text/html; charset=utf-8
```